

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-078520

(43)Date of publication of application : 14.03.2003

(51)Int.Cl.

H04L 9/16
 G09C 5/00
 H04L 9/08
 H04N 7/08
 H04N 7/081
 // H04N 7/167

(21)Application number : 2001-269623

(71)Applicant : NIPPON TELEGR & TELEPH CORP
 <NTT>

(22)Date of filing : 06.09.2001

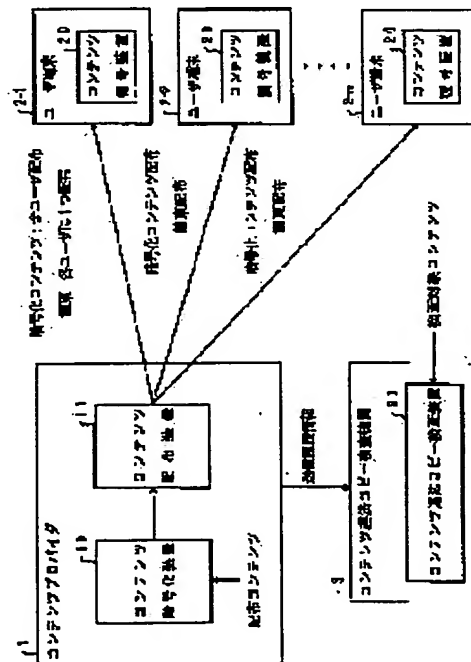
(72)Inventor : FUJII HIROSHI
 YASUDA HIROSHI

(54) CONTENTS ENCODING METHOD AND DEVICE, CONTENTS DECODING METHOD AND DEVICE, CONTENTS DISTRIBUTING METHOD AND DEVICE, CONTENTS ILLEGAL COPY CHECKING METHOD AND DEVICE, CONTENTS ENCRYPTING PROGRAM AND ITS PROGRAM RECORDING MEDIUM, CONTENTS DECODING PROGRAM AND ITS PROGRAM RECORDING MEDIUM, CONTENTS DISTRIBUTING PROGRAM AND ITS PROGRAM RECORDING MEDIUM, AND CONTENTS ILLEGAL COPY CHECKING PROGRAM AND ITS PROGRAM RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a technology for allowing a user side to efficiently embed user information in contents by using an electronic watermark, and for allowing a provider side to prevent the illegal cancel of the embodiment of electronic watermark information or the embodiment of any false electronic watermark information at the same time.

SOLUTION: Contents are divided into a plurality of parts, and a plurality of electronic watermarks are prepared for those respective divided parts, and the electronic watermark for each user is acquired by combining the values of the electronic watermarks of the extracted divided parts. Thus, it is possible for the user side to realize configuration that the electronic watermark information specific to the user is embedded in the contents, and it is possible for a provider side to actually control the electronic watermark information to be embedded and the embedding processing. Thus, it is possible to prevent the illegal cancel of the embodiment of the electronic watermark information or the embodiment of any false electronic watermark information at the user side.



LEGAL STATUS

[Date of request for examination]

08.10.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

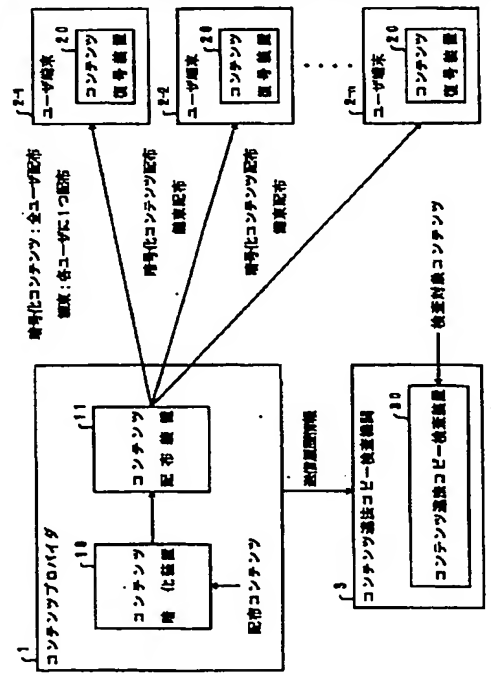
(19) 日本国特許庁 (JP) (12) 公開特許公報 (A) (11) 特許出願公開番号
特開2003-78520
(P2003-78520A)
(43) 公開日 平成15年3月14日 (2003.3.14)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 4 L 9/16		G 0 9 C 5/00	5 C 0 6 3
G 0 9 C 5/00		H 0 4 L 9/00	6 4 3 5 C 0 6 4
H 0 4 L 9/08			6 0 1 B 5 J 1 0 4
H 0 4 N 7/08		H 0 4 N 7/08	Z
7/081		7/167	Z
審査請求 未請求 請求項の数26 O L (全 21 頁) 最終頁に続く			

(21) 出願番号	特願2001-269623 (P2001-269623)	(71) 出願人	000004226 日本電信電話株式会社 東京都千代田区大手町二丁目3番1号
(22) 出願日	平成13年9月6日 (2001.9.6)	(72) 発明者	藤井 寛 東京都千代田区大手町二丁目3番1号 日 本電信電話株式会社内
		(72) 発明者	安田 浩 神奈川県横浜市栄区本郷台2丁目27番20号
		(74) 代理人	100087848 弁理士 小笠原 吉義 (外2名)
		最終頁に続く	

(54) 【発明の名称】 コンテンツ暗号化方法及び装置と、コンテンツ復号方法及び装置と、コンテンツ配布方法及び装置と、コンテンツ違法コピー検査方法及び装置と、コンテンツ暗号化プログラム及びそのプログ

(57) 【要約】
【課題】 本発明は、利用者側で電子透かしを使って利用者情報をコンテンツへ効率よく埋め込みながら、電子透かし情報の埋め込みの不正なキャンセルや、偽の電子透かし情報の埋め込みを防止できるようにする技術の提供を目的とする。
【解決手段】 コンテンツを複数の部分に分割して、それぞれの分割部分に対して複数の電子透かしを用意し、個々のユーザに対する電子透かしを、抽出された分割部分の電子透かしの値の組み合わせとするという構成を採る。これにより、ユーザ側で、ユーザに固有な電子透かし情報をコンテンツに埋め込むという形態をとりつつ、そのとき埋め込む電子透かし情報とその埋め込み処理とについては、実際には提供側で制御するようにしており、これにより、ユーザ側で、電子透かし情報の埋め込みを不正にキャンセルしたり、偽の電子透かし情報が埋め込まれることを防止できるようになる。



【特許請求の範囲】

【請求項 1】 コンテンツに電子透かし情報を埋め込んで暗号化するコンテンツ暗号化方法において、コンテンツを複数の部分に分割する過程と、上記分割した部分の全て又は一部を処理対象として、処理対象の分割部分のそれぞれに対して、複数の異なる電子透かし情報を埋め込む過程と、上記電子透かし情報の埋め込まれた分割部分及びその埋め込みの行われなかった分割部分を、別々の暗号鍵を使って暗号化する過程とを備えることを、特徴とするコンテンツ暗号化方法。

【請求項 2】 請求項 1 に記載のコンテンツ暗号化方法において、上記電子透かし情報を埋め込む過程では、上記処理対象とならなかった分割部分については、電子透かし情報を埋め込まないように処理することを、特徴とするコンテンツ暗号化方法。

【請求項 3】 請求項 1 に記載のコンテンツ暗号化方法において、上記電子透かし情報を埋め込む過程では、上記処理対象とならなかった分割部分については、固定的となる特定の電子透かし情報を埋め込むように処理することを、特徴とするコンテンツ暗号化方法。

【請求項 4】 請求項 1 ないし 3 のいずれか 1 項に記載のコンテンツ暗号化方法において、各分割部分に対して用いられた暗号鍵の集合の中から、各分割部分ごとに 1 つずつ暗号鍵を選択することで、暗号化されたコンテンツの復号に用いられる鍵束を生成する過程を備えることを、特徴とするコンテンツ暗号化方法。

【請求項 5】 コンテンツに電子透かし情報を埋め込んで暗号化するコンテンツ暗号化装置において、コンテンツを複数の部分に分割する手段と、上記分割した部分の全て又は一部を処理対象として、処理対象の分割部分のそれぞれに対して、複数の異なる電子透かし情報を埋め込む手段と、上記電子透かし情報の埋め込まれた分割部分及びその埋め込みの行われなかった分割部分を、別々の暗号鍵を使って暗号化する手段とを備えることを、特徴とするコンテンツ暗号化装置。

【請求項 6】 全て又は一部の分割部分のそれぞれに対して複数の異なる電子透かし情報が埋め込まれるとともに、その埋め込みの行われた分割部分及びその埋め込みの行われなかった分割部分が別々の暗号鍵を使って暗号化されることで生成される暗号化コンテンツの集合を復号対象として、暗号化コンテンツを復号するコンテンツ復号方法であって、各分割部分に対して用いられた暗号鍵の集合の中から、各分割部分ごとに 1 つずつ暗号鍵が選択されることで構成される鍵束の 1 つを取得する過程と、

上記鍵束を構成する各暗号鍵に対応付けられる暗号化コンテンツ部分を取り出す過程と、上記取り出した暗号化コンテンツ部分を、それに対応付けられる暗号鍵で復号する過程と、上記復号したコンテンツ部分を統合することでコンテンツを復元する過程とを備えることを、特徴とするコンテンツ復号方法。

【請求項 7】 全て又は一部の分割部分のそれぞれに対して複数の異なる電子透かし情報が埋め込まれるとともに、その埋め込みの行われた分割部分及びその埋め込みの行われなかった分割部分が別々の暗号鍵を使って暗号化されることで生成される暗号化コンテンツの集合を復号対象として、暗号化コンテンツを復号するコンテンツ復号装置であって、各分割部分に対して用いられた暗号鍵の集合の中から、各分割部分ごとに 1 つずつ暗号鍵が選択されることで構成される鍵束の 1 つを取得する手段と、上記鍵束を構成する各暗号鍵に対応付けられる暗号化コンテンツ部分を取り出す手段と、上記取り出した暗号化コンテンツ部分を、それに対応付けられる暗号鍵で復号する手段と、上記復号したコンテンツ部分を統合することでコンテンツを復元する手段とを備えることを、特徴とするコンテンツ復号装置。

【請求項 8】 電子透かし情報の埋め込まれた暗号化コンテンツを配布するコンテンツ配布方法において、コンテンツを複数の部分に分割する過程と、上記分割した部分の全て又は一部を処理対象として、処理対象の分割部分のそれぞれに対して、複数の異なる電子透かし情報を埋め込む過程と、上記電子透かし情報の埋め込まれた分割部分及びその埋め込みの行われなかった分割部分を、別々の暗号鍵を使って暗号化する過程と、各分割部分に対して用いられた暗号鍵の集合の中から、各分割部分ごとに 1 つずつ暗号鍵を選択することで構成される鍵束を生成する過程と、上記暗号化した分割部分の集合で構成される暗号化コンテンツを全ての配布先に配布する過程と、上記鍵束を 1 つ選択して、その選択した上記鍵束の暗号化したものを配布先に配布する過程とを備えることを、特徴とするコンテンツ配布方法。

【請求項 9】 請求項 8 に記載のコンテンツ配布方法において、配布先と、その配布先に配布した上記鍵束との対応関係を配布記録として記録するか、配布先と、その配布先に配布した上記鍵束により復号されるコンテンツから読み出される電子透かし情報との対応関係を配布記録として記録する過程を備えることを、特徴とするコンテンツ配布方法。

【請求項 10】 請求項 8 又は 9 に記載のコンテンツ配

布方法において、
上記鍵束と、それにより復号されるコンテンツから読み出される電子透かし情報との対応関係のリストを生成する過程を備えることを、
特徴とするコンテンツ配布方法。

【請求項 11】 請求項 8 又は 9 に記載のコンテンツ配布方法において、
コンテンツに埋め込まれるべき電子透かし情報が与えられるときに、規定の変換に従って、その埋め込みを実現する上記鍵束を求めることで、上記鍵束と、それにより復号されるコンテンツから読み出される電子透かし情報との対応関係を動的に特定する過程を備えることを、
特徴とするコンテンツ配布方法。

【請求項 12】 請求項 10 又は 11 に記載のコンテンツ配布方法において、
上記鍵束を配布する過程では、配布先 ID から求められる電子透かし情報を選択し、上記対応関係に従って、その電子透かし情報に対応付けられる上記鍵束を選択して、それを配布先に配布するように処理することを、
特徴とするコンテンツ配布方法。

【請求項 13】 請求項 10 又は 11 に記載のコンテンツ配布方法において、
上記鍵束を配布する過程では、未発行の電子透かし情報を選択し、上記対応関係に従って、その電子透かし情報に対応付けられる上記鍵束を選択して、それを配布先に配布するように処理することを、
特徴とするコンテンツ配布方法。

【請求項 14】 電子透かし情報の埋め込まれた暗号化コンテンツを配布するコンテンツ配布装置において、
コンテンツを複数の部分に分割する手段と、
上記分割した部分の全て又は一部を処理対象として、処理対象の分割部分のそれぞれに対して、複数の異なる電子透かし情報を埋め込む手段と、
上記電子透かし情報の埋め込まれた分割部分及びその埋め込みの行われなかった分割部分を、別々の暗号鍵を使って暗号化する手段と、
各分割部分に対して用いられた暗号鍵の集合の中から、各分割部分ごとに 1 つずつ暗号鍵を選択することで構成される鍵束を生成する手段と、
上記暗号化した分割部分の集合で構成される暗号化コンテンツを全ての配布先に配布する手段と、
上記鍵束を 1 つ選択して、その選択した上記鍵束の暗号化したものを配布先に配布する手段とを備えることを、
特徴とするコンテンツ配布装置。

【請求項 15】 全て又は一部の分割部分のそれぞれに対して複数の異なる電子透かし情報が埋め込まれるとともに、その埋め込みの行われた分割部分及びその埋め込みの行われなかった分割部分が別々の暗号鍵を使って暗号化されて配布され、更に、各分割部分ごとに 1 つずつ該暗号鍵が選択されることで構成される鍵束を使って復

号されるコンテンツを検査対象として、コンテンツの違法コピーを検査するコンテンツ違法コピー検査方法であって、

検査対象のコンテンツに埋め込まれる電子透かし情報を読み取る過程と、

上記読み取った電子透かし情報をキーにして、コンテンツの配布先ユーザと、その配布先ユーザに配布された上記鍵束により復号されるコンテンツから読み出される電子透かし情報との対応関係について記述するリストを参照することで、検査対象のコンテンツの正規の配布先ユーザを特定する過程と、

上記特定した正規の配布先ユーザと、検査対象のコンテンツを所有するユーザとが一致するの否かを検査する過程とを備えることを、
特徴とするコンテンツ違法コピー検査方法。

【請求項 16】 全て又は一部の分割部分のそれぞれに対して複数の異なる電子透かし情報が埋め込まれるとともに、その埋め込みの行われた分割部分及びその埋め込みの行われなかった分割部分が別々の暗号鍵を使って暗号化されて配布され、更に、各分割部分ごとに 1 つずつ該暗号鍵が選択されることで構成される鍵束を使って復号されるコンテンツを検査対象として、コンテンツの違法コピーを検査するコンテンツ違法コピー検査方法であって、

検査対象のコンテンツに埋め込まれる電子透かし情報を読み取る過程と、

上記読み取った電子透かし情報の埋め込みを実現する上記鍵束を特定する過程と、

上記特定した鍵束をキーにして、コンテンツの配布先ユーザと、その配布先ユーザに配布された上記鍵束との対応関係について記述するリストを参照することで、検査対象のコンテンツの正規の配布先ユーザを特定する過程と、

上記特定した正規の配布先ユーザと、検査対象のコンテンツを所有するユーザとが一致するの否かを検査する過程とを備えることを、

特徴とするコンテンツ違法コピー検査方法。

【請求項 17】 全て又は一部の分割部分のそれぞれに対して複数の異なる電子透かし情報が埋め込まれるとともに、その埋め込みの行われた分割部分及びその埋め込みの行われなかった分割部分が別々の暗号鍵を使って暗号化されて配布され、更に、各分割部分ごとに 1 つずつ該暗号鍵が選択されることで構成される鍵束を使って復号されるコンテンツを検査対象として、コンテンツの違法コピーを検査するコンテンツ違法コピー検査装置であって、

検査対象のコンテンツに埋め込まれる電子透かし情報を読み取る手段と、

上記読み取った電子透かし情報をキーにして、コンテンツの配布先ユーザと、その配布先ユーザに配布された上

記鍵束により復号されるコンテンツから読み出される電子透かし情報との対応関係について記述するリストを参照することで、検査対象のコンテンツの正規の配布先ユーザを特定する手段と、

上記特定した正規の配布先ユーザと、検査対象のコンテンツを所有するユーザとが一致するの否かを検査する手段とを備えることを、

特徴とするコンテンツ違法コピー検査装置。

【請求項 18】 全て又は一部の分割部分のそれぞれに対して複数の異なる電子透かし情報が埋め込まれるとともに、その埋め込みの行われた分割部分及びその埋め込みの行われなかった分割部分が別々の暗号鍵を使って暗号化されて配布され、更に、各分割部分ごとに1つずつ該暗号鍵が選択されることで構成される鍵束を使って復号されるコンテンツを検査対象として、コンテンツの違法コピーを検査するコンテンツ違法コピー検査装置であって、

検査対象のコンテンツに埋め込まれる電子透かし情報を読み取る手段と、

上記読み取った電子透かし情報の埋め込みを実現する上記鍵束を特定する手段と、

上記特定した鍵束をキーにして、コンテンツの配布先ユーザと、その配布先ユーザに配布された上記鍵束との対応関係について記述するリストを参照することで、検査対象のコンテンツの正規の配布先ユーザを特定する手段と、

上記特定した正規の配布先ユーザと、検査対象のコンテンツを所有するユーザとが一致するの否かを検査する手段とを備えることを、

特徴とするコンテンツ違法コピー検査装置。

【請求項 19】 請求項 1 ないし 4 のいずれか 1 項に記載のコンテンツ暗号化方法の実現に用いられる処理をコンピュータに実行させるためのコンテンツ暗号化プログラム。

【請求項 20】 請求項 1 ないし 4 のいずれか 1 項に記載のコンテンツ暗号化方法の実現に用いられる処理をコンピュータに実行させるためのプログラムを記録したコンテンツ暗号化プログラムの記録媒体。

【請求項 21】 請求項 6 に記載のコンテンツ復号方法の実現に用いられる処理をコンピュータに実行させるためのコンテンツ復号プログラム。

【請求項 22】 請求項 6 に記載のコンテンツ復号方法の実現に用いられる処理をコンピュータに実行させるためのプログラムを記録したコンテンツ復号プログラムの記録媒体。

【請求項 23】 請求項 8 ないし 13 のいずれか 1 項に記載のコンテンツ配布方法の実現に用いられる処理をコンピュータに実行させるためのコンテンツ配布プログラム。

【請求項 24】 請求項 8 ないし 13 のいずれか 1 項に

記載のコンテンツ配布方法の実現に用いられる処理をコンピュータに実行させるためのプログラムを記録したコンテンツ配布プログラムの記録媒体。

【請求項 25】 請求項 15 又は 16 に記載のコンテンツ違法コピー検査方法の実現に用いられる処理をコンピュータに実行させるためのコンテンツ違法コピー検査プログラム。

【請求項 26】 請求項 15 又は 16 に記載のコンテンツ違法コピー検査方法の実現に用いられる処理をコンピュータに実行させるためのプログラムを記録したコンテンツ違法コピー検査プログラムの記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンテンツに電子透かし情報を埋め込んで暗号化するコンテンツ暗号化方法及び装置と、その暗号化技術により暗号化されたコンテンツを復号するコンテンツ復号方法及び装置と、その暗号化技術により暗号化されたコンテンツを配布するコンテンツ配布方法及び装置と、その暗号化技術により暗号化されたコンテンツの違法コピーを検査するコンテンツ違法コピー検査方法及び装置と、そのコンテンツ暗号化方法の実現に用いられるコンテンツ暗号化プログラム及びそのプログラムを記録した記録媒体と、そのコンテンツ復号方法の実現に用いられるコンテンツ復号プログラム及びそのプログラムを記録した記録媒体と、そのコンテンツ配布方法の実現に用いられるコンテンツ配布プログラム及びそのプログラムの記録媒体と、そのコンテンツ違法コピー検査方法の実現に用いられるコンテンツ違法コピー検査プログラム及びそのプログラムを記録した記録媒体とに関する。

【0002】

【従来の技術】ディジタルデータは劣化なくコピーが作成可能で、ネットワークを用いた再配布が容易という特徴をもつ。これへの対策として用いられるのが電子透かしである。電子透かしは、画像や音声などのコンテンツに人間の視覚や聴覚では認識困難な形で別の情報を埋め込む手法である。

【0003】電子透かしのコンテンツ保護への利用法のひとつは、コンテンツの著作権に関わる情報を埋め込む方式である。これはコンテンツの著者名や識別子を電子透かしして埋め込み、コピー配布時に、この情報によって正当な権利の主張を可能にするものである。

【0004】しかしながら、この著作権に関わる情報の埋め込みによる保護は、電子透かしから違法コピーを行ったものに関する情報は得られず、違法コピー対策の効果は弱い。

【0005】第2の電子透かし利用法は、電子透かしとしてコンテンツの利用者に関する情報を埋め込むものである。これはコンテンツを利用者に販売または譲渡した場合に、その利用者の情報がコンテンツに電子透かしと

して埋め込まれるようにする。

【0006】この場合、違法コピーされたコンテンツに埋め込まれた電子透かしの情報から、コンテンツが当初販売または譲渡されたユーザが識別可能となり、違法コピーの流出経路に関する情報が得られるため、違法コピー対策が著作権に関わる情報を埋め込む場合より高い。

【0007】一方、著作権情報を埋め込む場合には、同一コンテンツに埋め込むべき電子透かし情報は唯一であるため、同一電子透かしの埋め込まれたデータの大量コピーを配布することが可能である。

【0008】これに対して、利用者情報を埋め込む場合には、同一コンテンツに埋め込む場合であっても電子透かし情報は配布先の利用者ごとに異なり、配布先ごとに新たなコンテンツデータを生成する必要がある。これはコンテンツ提供者にとって非常に負荷が大きいのみならず、CD-ROMや放送といったコンテンツの一括の大量流通が不可能となるという問題を発生させる。

【0009】本出願人が開示した特開平10-191025号に記載される発明では、これを解決するために、電子透かしの埋め込みを利用者側で行う方法を提案している。

【0010】この発明では、コンテンツをスクランブルして利用者に送付し、これとは別に、スクランブル解除鍵と電子透かしとして埋め込む利用者情報とを合成したデータを利用者に送付する。利用者はコンテンツを利用する場合にスクランブルを解除するが、スクランブル解除器には電子透かし埋め込み機能を持たせており、スクランブル解除鍵と同時に、送付した利用者情報を電子透かしを使ってスクランブルを解除したコンテンツに埋め込む。

【0011】これによって電子透かしの埋め込みをコンテンツ利用者に行わせることが可能となり、コンテンツ提供者の負荷を低減させるとともに、CD-ROMや放送によるコンテンツ配布との両立を可能にしている。

【0012】

【発明が解決しようとする課題】しかしながら、この方式（特開平10-191025号に記載される発明の方式）では、スクランブル解除と透かし埋め込みの二つの処理から構成されるため、スクランブル解除を行う処理のみを不正に抽出された場合、電子透かしの埋め込まれていないコンテンツが生成される危険性がある。

【0013】また、この方式では、利用者に送付される情報の中に透かしとして埋め込まれるべき情報が含まれるため、送付された利用者情報が電子透かしとして埋め込まれる前の段階で改ざんされた場合、偽の利用者情報がコンテンツに埋め込まれる可能性がある。

【0014】本発明は、このような問題を解決するためのものであり、利用者情報の電子透かしとしてのコンテンツへの埋め込みを利用者側で効率よく行いながら、利用者側で電子透かし情報の埋め込みを不正にキャンセルしたり、偽の電子透かし情報が埋め込まれることを防止

できるようにする新たな電子透かし情報の埋め込み技術の提供を目的とする。

【0015】

【課題を解決するための手段】図1に、本発明を具備するシステム構成の一例を図示する。

【0016】図中、1は本発明を具備するコンテンツプロバイダ、2-i（ $i=1\sim n$ ）は本発明を具備するユーザ端末、3は本発明を具備するコンテンツ違法コピー検査機関である。

【0017】本発明を具備するコンテンツプロバイダ1は、本発明のコンテンツ暗号化装置10と本発明のコンテンツ配布装置11とを備え、本発明を具備するユーザ端末2-iは、本発明のコンテンツ復号装置20を備え、本発明を具備するコンテンツ違法コピー検査機関3は、本発明のコンテンツ違法コピー検査装置30を備える。

【0018】（1）コンテンツ暗号化装置10の構成
本発明のコンテンツ暗号化装置10は、暗号化対象のコンテンツを処理対象として、①コンテンツを複数の部分に分割する手段と、②その分割した部分の全て又は一部を処理対象として、処理対象の分割部分のそれぞれに対して、複数の異なる電子透かし情報を埋め込む手段と、③電子透かし情報の埋め込まれた分割部分及びその埋め込みの行われなかった分割部分を、別々の暗号鍵を使って暗号化する手段と、④各分割部分に対して用いられた暗号鍵の集合の中から、各分割部分ごとに1つずつ暗号鍵を選択することで、暗号化されたコンテンツの復号に用いられる鍵束を生成する手段とを備えるように構成する。

【0019】（2）コンテンツ復号装置20の構成
本発明のコンテンツ復号装置20は、本発明のコンテンツ暗号化装置10が生成した暗号化コンテンツの集合を復号対象として、①本発明のコンテンツ暗号化装置10が生成した鍵束の1つを取得する手段と、②その取得した鍵束を構成する各暗号鍵に対応付けられる暗号化コンテンツ部分を取り出す手段と、③その取り出した暗号化コンテンツ部分を、それに対応付けられる暗号鍵で復号する手段と、④その復号したコンテンツ部分を統合することでコンテンツを復元する手段とを備えるように構成する。

【0020】ここで、本発明のコンテンツ復号装置20は、コンテンツプロバイダ1から配布されてくる鍵束が暗号化されていることに対応して、それを復号する手段を備えることになる。

【0021】（3）コンテンツ配布装置11の構成
本発明のコンテンツ配布装置11は、本発明のコンテンツ暗号化装置10が生成した暗号化コンテンツの集合を配布対象として、本発明のコンテンツ暗号化装置10が備えられる場合には、①本発明のコンテンツ暗号化装置10が生成した暗号化コンテンツの集合を全ての配布先に配布する手段と、②本発明のコンテンツ暗号化装置1

0 が生成した鍵束を 1 つ選択して、その選択した鍵束の暗号化したものを配布先に配布する手段とを備える。一方、本発明のコンテンツ暗号化装置 10 が備えられない場合には、この 2 つの手段の他に、本発明のコンテンツ暗号化装置 10 の備える各手段を備えるように構成する。

【0022】更に、本発明のコンテンツ配布装置 11 は、③配布先と、その配布先に配布した鍵束との対応関係を配布記録として記録するか、配布先と、その配布先に配布した鍵束により復号されるコンテンツから読み出される電子透かし情報との対応関係を配布記録として記録する手段を備えたり、④鍵束と、それにより復号されるコンテンツから読み出される電子透かし情報との対応関係のリストを生成する手段を備えたり、⑤コンテンツに埋め込まれるべき電子透かし情報が与えられるときに、規定の変換に従って、その埋め込みを実現する鍵束を求めることで、鍵束と、それにより復号されるコンテンツから読み出される電子透かし情報との対応関係を動的に特定する手段を備えることがある。

【0023】(4) コンテンツ違法コピー検査装置 30 の構成

本発明のコンテンツ違法コピー検査装置 30 は、本発明のコンテンツ復号装置 20 が復号したコンテンツを検査対象として、①検査対象のコンテンツに埋め込まれる電子透かし情報を読み取る手段と、②その読み取った電子透かし情報をキーにして、本発明のコンテンツ配布装置 11 が配布記録として記録した対応関係のリスト（コンテンツの配布先ユーザと、その配布先ユーザに配布した鍵束により復号されるコンテンツから読み出される電子透かし情報との対応関係のリスト）を参照することで、検査対象のコンテンツの正規の配布先ユーザを特定する手段と、③その特定した正規の配布先ユーザと、検査対象のコンテンツを所有するユーザとが一致するの否かを検査する手段とを備えるように構成する。

【0024】ここで、リストを参照する手段は、本発明のコンテンツ配布装置 11 からそのリストを取得して参照することもあるし、本発明のコンテンツ配布装置 11 に問い合わせることによってそのリストを参照することもある。

【0025】また、本発明のコンテンツ違法コピー検査装置 30 は、本発明のコンテンツ復号装置 20 が復号したコンテンツを検査対象として、①検査対象のコンテンツに埋め込まれる電子透かし情報を読み取る手段と、②規定の変換を施したり、本発明のコンテンツ配布装置 11 が生成した対応関係のリスト（鍵束と、それにより復号されるコンテンツから読み出される電子透かし情報との対応関係のリスト）を参照することにより、その読み取った電子透かし情報の埋め込みを実現する鍵束を特定する手段と、③その特定した鍵束をキーにして、本発明のコンテンツ配布装置 11 が配布記録として記録した対

応関係のリスト（コンテンツの配布先ユーザと、その配布先ユーザに配布した鍵束との対応関係のリスト）を参照することで、検査対象のコンテンツの正規の配布先ユーザを特定する手段と、④その特定した正規の配布先ユーザと、検査対象のコンテンツを所有するユーザとが一致するの否かを検査する手段とを備えるように構成する。

【0026】ここで、リストを参照する手段は、本発明のコンテンツ配布装置 11 からそのリストを取得して参照することもあるし、本発明のコンテンツ配布装置 11 に問い合わせることによってそのリストを参照することもある。

【0027】このように構成される本発明のコンテンツ配布装置 11（本発明のコンテンツ暗号化装置 10）では、例えば、図 2 に示すように、コンテンツ c を L 個の (c_1, c_2, \dots, c_L) に分割して、その L 個の各分割部分 c_i に対して、例えば、電子透かし操作 $w_{i,j}$ (i は分割部分の識別子、 j は埋め込む電子透かし情報の識別子) を使って電子透かし情報 “0”, “1” を埋め込んでから、暗号鍵 $k_{i,j}$ (i は分割部分の識別子、 j は電子透かし情報の識別子) を使って暗号化することで、それらの暗号化コンテンツの集合で構成されるコンテンツ配布用データを生成するとともに、それらの暗号鍵 $k_{i,j}$ から、 L 個の各分割部分 c_i ごとに 1 つずつ暗号鍵 $k_{i,j}$ を選択することで、コンテンツ c の復号に用いられる鍵束 K_j ($j = 1 \sim 2^L$) を生成する。

【0028】このとき、本発明のコンテンツ配布装置 11 は、鍵束 K_j と、それにより復号されるコンテンツから読み出される電子透かし情報 d_j (図 2 の例では “0” と “1” の羅列データ) との対応関係のリストを生成する。

【0029】続いて、本発明のコンテンツ配布装置 11 は、図 3 に示すように、全てのユーザ端末 2- i (図 3 の例では 8 台のユーザ端末) に対して、生成したコンテンツ配布用データを配布するとともに、各ユーザ端末 2- i に対して、1 つずつ鍵束 K_j を選択して、その選択した鍵束 K_j の暗号化したものを配布する。

【0030】この鍵束 K_j の選択処理は、例えば、配布先ユーザの ID から求められる電子透かし情報 (例えば、ID の 2 進数表現に対応付けられる電子透かし情報 d_j) を選択し、生成してある鍵束 K_j と電子透かし情報 d_j との対応関係のリストに従って、その電子透かし情報に対応付けられる鍵束を選択することで行ったり、未発行の電子透かし情報を選択し、生成してある鍵束 K_j と電子透かし情報 d_j との対応関係のリストに従って、その電子透かし情報に対応付けられる鍵束を選択することで行う。

【0031】ここで、鍵束 K_j と電子透かし情報 d_j との対応関係のリストを予め生成しておかず、電子透かし情報 d_j が与えられるときに、規定の変換に従って、

その電子透かし情報 d_j の埋め込みを実現する鍵束 K_j を動的に特定するようにしてもよい。例えば、“00000000”という電子透かし情報 d_j が与えられるときには、図2の例で説明するならば、“0”が8個並ぶことで、その電子透かし情報 d_j の埋め込みを実現する鍵束 K_j は、

$$K_j = k_{1,1}, k_{2,1}, k_{3,1}, \dots, k_{L,1}$$

であるというように、その時点で、与えられた電子透かし情報 d_j に対応付けられる鍵束 K_j を動的に特定するようにしてもよいのである。

【0032】このような配布処理を行うときに、本発明のコンテンツ配布装置11は、本発明のコンテンツ違法コピー検査装置30によるコンテンツ違法コピー検査を可能ならしめるために、図3に示すように、その配布記録として、配布先ユーザのIDと、その配布先ユーザに配布した鍵束 K_j との対応関係を記録したり、配布先ユーザのIDと、その配布先ユーザに配布した鍵束 K_j により復号されるコンテンツから読み出される電子透かし情報 d_j （図3の例では“0”と“1”の羅列データ）との対応関係を記録する。

【0033】一方、本発明のコンテンツ復号装置20は、本発明のコンテンツ配布装置11から配布される鍵束を受けて、受信してあるコンテンツ配布用データから、その鍵束を構成する各暗号鍵に対応付けられる暗号化コンテンツ部分を取り出し、その取り出した暗号化コンテンツ部分を、それに対応付けられる暗号鍵で復号して、その復号したコンテンツ部分を統合することでコンテンツを復元する。

【0034】このようにして復元されるコンテンツには、配布される鍵束に従って、配布先ユーザに固有な電子透かし情報が埋め込まれることになる。しかも、この配布先ユーザに固有な電子透かし情報の埋め込みは、配布先のユーザ側で行われることになる。

【0035】一方、本発明のコンテンツ違法コピー検査装置30は、検査対象のコンテンツが与えられると、そのコンテンツに埋め込まれる電子透かし情報を読み取り、それをキーにして、本発明のコンテンツ配布装置11が記録した配布記録のリスト（コンテンツの配布先ユーザと、その配布先ユーザに配布された鍵束により復号されるコンテンツから読み出される電子透かし情報との対応関係のリスト）を参照することで、検査対象のコンテンツの正規の配布先ユーザを特定して、それによって、検査対象のコンテンツを所有するユーザが正規のコンテンツ所有者であるのかを検査する。

【0036】また、本発明のコンテンツ違法コピー検査装置30では、検査対象のコンテンツが与えられると、そのコンテンツに埋め込まれる電子透かし情報を読み取り、規定の変換を施すことなどにより、その読み取った電子透かし情報の埋め込みを実現する鍵束を特定して、それをキーにして、本発明のコンテンツ配布装置11が

記録した配布記録のリスト（コンテンツの配布先ユーザと、その配布先ユーザに配布された鍵束との対応関係のリスト）を参照することで、検査対象のコンテンツの正規の配布先ユーザを特定して、それによって、検査対象のコンテンツを所有するユーザが正規のコンテンツ所有者であるのかを検査する。

【0037】このようにして検査されるコンテンツには、正規のコンテンツ所有者に固有の電子透かし情報が埋め込まれており、これにより、コンテンツ所有者が正規の所有者であるのか否かということと、コンテンツの不正コピーが行われた場合には、どの正規のコンテンツ所有者の所有するコンテンツからコピーが行われたのかということを検出できるようになる。

【0038】このようにして、本発明では、ユーザ側で、ユーザに固有な電子透かし情報をコンテンツに埋め込むという形態をとりつつ、そのとき埋め込む電子透かし情報とその埋め込み処理については、実際には鍵束を使って提供側で制御するようにしており、これにより、ユーザ側で、電子透かし情報の埋め込みを不正にキャンセルしたり、偽の電子透かし情報が埋め込まれることを防止できるようになる。

【0039】そして、コンテンツの不正コピーが行われる場合に、それを正確に検出できるとともに、そのコピー元を正確に検出できるようになる。

【0040】以上に説明したように、本発明では、コンテンツを複数の部分に分割して、それぞれの分割部分に対して複数の電子透かしを用意し、個々のユーザに対する電子透かしを、抽出された分割部分の電子透かしの値の組み合わせとするという構成を採っており、これにより、電子透かし入りコンテンツとして用意すべきデータ量を少なくできるようになる。

【0041】すなわち、従来行われていたように、コンテンツに直接、利用者情報を電子透かしとして埋め込む場合、 n 人の利用者に対しては n 通りに電子透かしを埋め込む必要があり、提供者での電子透かし埋め込み回数は n 回となる。元のコンテンツのデータ量を C とすると、電子透かしによるデータ量増加がないと仮定しても、電子透かし入りコンテンツのデータ量の合計は $C \times n$ である。これでは、利用者が増加するにつれて、膨大な埋め込み回数になるとともに、膨大なデータ量になる。

【0042】このように、従来技術に従っていると、電子透かし埋め込み回数の問題から、提供者の負荷が大きく、また、データ量の問題から、予め用意したコンテンツのCD-ROMや放送などによる一括の配布が不可能となっている。

【0043】これに対して本発明の方式では、コンテンツから m 個の部分抽出し、各部分に k 種類の電子透かしデータに対応させる場合、コンテンツ全体で $k \times m$ 種類の電子透かしが埋め込める。 n 人の利用者に対しては、

およそ、「 $k \times \log n \div \log k$ 」回の電子透かし埋め込みとなり、 n に比べて非常に少ない。また、 n 人の利用者すべてを区別する電子透かしの組み合わせを実現するためのデータ量も、これに比例するため、 $C \times n$ に比べて非常に少ない。

【0044】さらに、抽出部分の合計 C' （本発明の電子透かし埋め込み処理の対象となる部分の合計）をコンテンツのデータ量 C に比べて小さくすると、異なる利用者のための電子透かしを埋め込んだデータを予め用意するためのデータ量が「 $C' \times \log n \div \log k$ 」となり、オリジナルコンテンツ C に比べて n 人の利用者用の電子透かし情報追加のためのデータ量が小さく、予め全利用者用の電子透かし入りコンテンツを用意してCD-ROMなどによる一括配布や、放送やサーバからのダウンロードによる一括配布などが可能となる。

【0045】

【発明の実施の形態】以下、実施の形態に従って本発明を詳細に説明する。

【0046】本発明の説明に入る前に、数学的な準備を行う。

【0047】コンテンツの符号化の形式 F に対して、次のような性質を満たす分割操作 Ω とその逆変換とを用意する。ここでいう形式 F とは、画像符号化におけるビットマップ符号化やJPEG、動画符号化におけるMPEG、音声符号化におけるMP3などをさす。

【0048】(1) [性質 Ω : Ω の性質]

形式 F で符号化されたコンテンツ c は、分割操作 Ω によって複数(L 個)の部分 c_1, c_2, \dots, c_L に分割される。これを $C = \Omega(c)$ と書くことにする。ここで、 C は分割部分の系列で、 $C = c_1, c_2, \dots, c_L$ である。

【0049】分割操作 Ω は、その逆変換 Ω' （結合操作と呼ぶ）が定義できて、 Ω' を分割された部分の系列 $C = c_1, c_2, \dots, c_L$ に適用することによって、形式 F を満たすコンテンツ c' を生成できる。これを $c' = \Omega'(C)$ または $c' = \Omega'(c_1, c_2, \dots, c_L)$ と書くことにする。（この性質の説明終了）。

【0050】次に、形式 F 、操作 Ω に対して、以下ののような性質を満たす、コンテンツの分割部分に対する操作（電子透かし操作になる）の集合の系列

$W = w_1, w_2, \dots, w_L$

但し、 $w_i = (w_{i,1}, w_{i,2}, \dots, w_{i,N_i})$ ($i = 1 \sim L$)

を用意する。

【0051】(2) [性質 $W1$: W の性質]

Ω によって行われるコンテンツの分割による i 番目 ($i = 1, 2, \dots, L$) の分割部分のそれぞれに対して、操作の集合 v_i を対応させる。 Ω によるコンテンツ c の i 番目の分割部分 c_i に、 v_i 中の任意の操作 $w_{i,k}$ を適用することで得られたデータを $w_{i,k}(c_i)$ とする。

【0052】ここで、 v_i ($i = 1, 2, \dots, L$) の中か

ら、各 i に対して任意の操作 $w_{i,k}$ を一つずつ選んで、各分割部分に対する操作の系列からなる「分割部分の系列に対する操作」

$W = w_1, k_1, w_2, k_2, \dots, w_L, k_L$

を作り、これを分割部分の系列 C に次のように適用する。

【0053】 $w(C) = w_1, k_1(c_1), w_2, k_2(c_2), \dots, w_L, k_L(c_L)$

このとき、これに Ω' を適用することで得られたデータ $c^W = \Omega'(w(C)) = \Omega'(w_1, k_1(c_1), w_2, k_2(c_2), \dots, w_L, k_L(c_L))$

は、もとのコンテンツ c が符号化形式 F を満足していれば、ふたたび F を満足する。（この性質の説明終了）。

【0054】符号化 F を満足するあるコンテンツ c と分割操作 Ω に対して、 W が次のような性質を満足するとき、 W は c に識別子を埋め込むと呼ぶことにし、 W 中の操作をそれぞれの対象への識別子埋め込み操作と呼ぶ。

【0055】(3) [性質 $W2$: W の性質]

W から取った、分割部分の系列に対する二つの操作 w_1, w_2

$w_1 = w_1, k_1, w_2, k_2, \dots, w_L, k_L$

$w_2 = w_1, m_1, w_2, m_2, \dots, w_L, m_L$

が一致しない、つまり、 w_1, w_2 中のある分割部分に対する操作 w_{j,k_j} と w_{j,m_j} とが異なる場合には、 c を分割して w_1 と w_2 とを適用して統合すると、異なったコンテンツデータが得られる。つまり、

$\Omega'(w_1(\Omega(c))) \neq \Omega'(w_2(\Omega(c)))$

となる。（この性質の説明終了）。

【0056】次に、識別子埋め込み操作 W に対して、以下のような二つの性質を満たす、コンテンツからのデータの読み取り操作 R （電子透かしの読み取り操作になる）を用意する。

【0057】(4) [性質 $R1$: R の性質]

一つの W からとられた任意の二つの異なる、分割部分の系列に対する異なる操作 w_1 と w_2 とに対して、 $R(\Omega'(w_1(\Omega(c)))) \neq R(\Omega'(w_2(\Omega(c))))$ が成立し、また、任意の分割部分の系列に対する操作 w に対して

$R(c) \neq R(\Omega'(w(\Omega(c))))$

が成立する。ここで、 $R(c)$ は、データを読み取れない($R(c) = \phi$ 、読み取りエラー)場合を含む。（この性質の説明終了）。

【0058】(5) [性質 $R2$: R によるデータのコンテンツに独立な読み取り]

ある W から取られた分割部分の系列に対する操作 w と、形式 F を満たす異なるコンテンツ c_a, c_b とが存在したとき

$R(\Omega'(w(\Omega(c_a)))) = R(\Omega'(w(\Omega(c_b))))$ となる。

【0059】すなわち、異なるコンテンツに同一の電子

透かし情報が埋め込まれた場合に、コンテンツからのデータの読み取り操作Rを施すことで、同一の電子透かし情報を読み出せることになる。(この性質の説明終了)。

【0060】コンテンツcにデータ読み取り操作Rを適用することで、あるデータ $d=R(c)$ が抽出できる。ここで、分割部分の系列に対する識別子埋め込み操作wのとり方は「 $N_1 \times N_2 \times \dots \times N_L$ 」種類ある。これから、操作 $\Omega'(w(\Omega(c)))$ によって、Rから読み出されるデータが異なるものとなる「 $N_1 \times N_2 \times \dots \times N_L$ 」個のコンテンツが得られることを示す。

【0061】また、Rが〔性質R2〕を満足するとき、wが同一であればコンテンツに関わらず同一のデータが読み出せることになる。(準備終了)。

【0062】以上のような準備のもとに、コンテンツの安全な配布について実現する本発明の一実施形態例について説明する。

【0063】ここで、以下の説明では、説明の便宜上、コンテンツに埋め込む電子透かし情報として、識別子のような目に見えるような情報を想定しているが、本発明はそのような電子透かし情報の埋め込みに限られるものではなくて、要するに、性質の異なるものをコンテンツに埋め込むことで構成される電子透かしに対して、そのまま適用できる。また、コンテンツも画像に限られるものでもない。

【0064】図4に、図1に示した本発明を具備するコンテンツプロバイダ1及びユーザ端末2の持つ機能構成の一実施形態例を図示し、図5に、図1に示した本発明を具備するコンテンツ違法コピー検査機関3の持つ機能構成の一実施形態例を図示する。

【0065】本発明を具備するコンテンツプロバイダ1は、図4に示すように、ユーザ端末2へコンテンツを送信するための暗号化されたコンテンツ配布用データを生成するコンテンツ配布用データ生成部100と、生成されたコンテンツ配布用データを保存するコンテンツ配布用データ格納部101と、保存されるコンテンツ配布用データをユーザ端末2に送信するコンテンツ配布用データ送信部102と、コンテンツ配布用データの復号に用いられる鍵束を生成する鍵束生成部103と、生成された鍵束とそれにより復号されるコンテンツから読み出される識別子(ユーザに固有な電子透かし情報)との対応関係を管理する鍵束識別子対応リスト104と、コンテンツに埋め込まれるべき識別子が与えられるときに、その埋め込みを実現する鍵束を動的に特定する識別子鍵束変換部105と、ユーザ端末2に送信する送信先に固有の鍵束を選択する鍵束選択部106と、選択された鍵束を暗号化してユーザ端末2に送信する鍵束送信部107と、ユーザ端末2に送信した鍵束の情報(ユーザIDと、送信した鍵束と、その鍵束により復号されるコンテンツから読み出される識別子との対応関係の情報)を保

存する配布記録格納部108とを備える。

【0066】ここで、このコンテンツ配布用データ生成部100やコンテンツ配布用データ送信部102や鍵束生成部103や識別子鍵束変換部105や鍵束選択部106や鍵束送信部107は、具体的にはコンピュータプログラムで実現されるものであり、これらのコンピュータプログラムは、計算機が読み取り可能な半導体メモリなどの適当な記録媒体に格納することができる。

【0067】一方、本発明を具備するユーザ端末2は、図4に示すように、コンテンツプロバイダ1から送信されてくるコンテンツ配布用データを受信するコンテンツ配布用データ受信部200と、受信されたコンテンツ配布用データを保存するコンテンツ配布用データ格納部201と、コンテンツプロバイダ1から送信されてくる暗号化された鍵束を受信して復号する鍵束受信部202と、受信された鍵束を使って、受信されたコンテンツ配布用データを復号することでコンテンツを復元するコンテンツ復元部203とを備える。

【0068】ここで、このコンテンツ配布用データ受信部200や鍵束受信部202やコンテンツ復元部203は、具体的にはコンピュータプログラムで実現されるものであり、これらのコンピュータプログラムは、計算機が読み取り可能な半導体メモリなどの適当な記録媒体に格納することができる。

【0069】一方、本発明を具備するコンテンツ違法コピー検査機関3は、図5に示すように、検査対象のコンテンツに埋め込まれる識別子(ユーザに固有な電子透かし情報)を読み出す識別子読出部300と、コンテンツプロバイダ1の持つ配布記録格納部108の情報を取得する取得部301と、取得された配布記録格納部108の情報(ユーザIDと識別子との対応関係の情報)を保存する配布記録格納部302と、取得された配布記録格納部108の情報(ユーザIDと鍵束との対応関係の情報)を保存する配布記録格納部303と、規定の変換を施したり、本発明を具備するコンテンツプロバイダ1が生成した鍵束識別子対応リスト104の情報を参照することで、検査対象のコンテンツから読み出された識別子に対応付けられる鍵束を特定する鍵束特定部304と、配布記録格納部302の情報を参照しつつ検査対象のコンテンツが違法コピーされたものであるのか否かを検査する違法コピー検査部305と、配布記録格納部303の情報を参照しつつ検査対象のコンテンツが違法コピーされたものであるのか否かを検査する違法コピー検査部306とを備える。

【0070】ここで、識別子読出部300や取得部301や鍵束特定部304や違法コピー検査部305や違法コピー検査部306は、具体的にはコンピュータプログラムで実現されるものであり、これらのコンピュータプログラムは、計算機が読み取り可能な半導体メモリなどの適当な記録媒体に格納することができる。

【0071】なお、この実施形態例では、コンテンツプロバイダ1からユーザ端末2にダウンロードすることでコンテンツを配布するという構成を探っているが、コンテンツの配布方法としては、放送やサーバなどからのダウンロードによる配布の他に、CD-ROMなどを使って配布する方法など様々なものがあり、本発明はそれらの配布方法に対して適用可能である。

【0072】(i) コンテンツプロバイダ1の処理の説明

(イ) コンテンツ配布用データ生成部100の処理
コンテンツ配布用データ生成部100は、図6の処理フローを実行することで、利用者へコンテンツを配布するためのコンテンツ配布用データを生成する処理を行う。

【0073】すなわち、先ず最初に、形式Fで符号化された配布対象となるコンテンツcに対して分割操作 Ω を施し、コンテンツの分割部分の系列 $C = c_1, c_2, \dots, c_L$ を生成する。

【0074】続いて、識別子埋め込み操作の集合Wを用意し、W内の各々の持つ分割部分に対する識別子埋め込み操作 $w_{i,j}$ を、Cの対応する分割部分 c_i に適用して、 $N_1 + N_1 + \dots + N_L$ 個の分割部分 $w_{1,1}(c_1), w_{1,2}(c_1), \dots, w_{1,N_1}(c_1), w_{2,1}(c_2), w_{2,2}(c_2), \dots, w_{2,N_2}(c_2), \dots, w_{L,1}(c_L), w_{L,2}(c_L), \dots, w_{L,N_L}(c_L)$ を生成する。

【0075】続いて、識別子の埋め込まれた $N_1 + N_1 + \dots + N_L$ 個の分割部分のそれぞれについて、別々の暗号鍵を用いて暗号化を行う。

【0076】これによって得られた $N_1 + N_1 + \dots + N_L$ 個の暗号化された分割部分の集まり、 $D = E(k_{1,1}, w_{1,1}(c_1)), E(k_{1,2}, w_{1,2}(c_1)), \dots, E(k_{1,N_1}, w_{1,N_1}(c_1)), E(k_{2,1}, w_{2,1}(c_2)), E(k_{2,2}, w_{2,2}(c_2)), \dots, E(k_{2,N_2}, w_{2,N_2}(c_2)), \dots, E(k_{L,1}, w_{L,1}(c_L)), E(k_{L,2}, w_{L,2}(c_L)), \dots, E(k_{L,N_L}, w_{L,N_L}(c_L))$ をコンテンツ配布用データとする。

【0077】ここで、 $k_{i,j}$ は暗号鍵を示し、 $E(k, \dots)$ は暗号鍵kによる暗号化を示しており、したがって、 $E(k_{i,j}, w_{i,j}(c_i))$ はCの分割部分 c_i に識別子を埋め込んで暗号化したデータを示している。

【0078】この暗号鍵の集合 $k_i = \{k_{i,1}, k_{i,2}, \dots, k_{i,N_i}\}$ は、分割部分 c_i に識別子を埋め込んで暗号化したデータに対する復号鍵の集合となる。これから、暗号鍵の集合 k_i を単に分割部分 c_i に対する鍵集合と呼ぶことにする。

【0079】最後に、この生成したコンテンツ配布用データをコンテンツ配布用データ格納部101に格納する。

【0080】この処理を実行するにあたって、コンテンツ配布用データ生成部100は、分割操作 Ω によってコンテンツcを(L個)の部分 c_1, c_2, \dots, c_L に分割するときに、部分 c_1 を主体部、それ以外の部分 c_2, \dots, c_L を調整部というように、それらの分割部分を性質の異なる二種類のクラスに分けて、主体部については識別子埋め込み操作を行わないように処理してもよい。

【0081】つまり、分割部分に対する操作集合において、 $v_1 = (w_{1,1}) = (1)$ (1は恒等変換)とすることで、主体部の c_1 に対しては操作を施さないように処理してもよい。このとき、 c_2, \dots, c_L のデータ量を c_1 のデータ量に比べて少なくとるように処理してもよい。

【0082】すなわち、コンテンツcの全ての部分に対して、本発明による識別子の埋め込み操作を行う必要はなく、また、電子透かしの埋め込みが難しいコンテンツ部分もあるので、例えば、そのようなコンテンツ部分を主体部として、その部分に対しては本発明による識別子埋め込み操作を行わないように処理するのである。

【0083】また、本発明による識別子の埋め込み操作を行うと、それに応じてコンテンツ配布用データのデータ量が大きくなるので、それを防止するために、このように主体部を設けて、主体部については本発明による識別子埋め込み操作を行わないように処理するのである。

【0084】この主体部について、本発明による識別子の埋め込み操作を行わないという構成を探るのではなくて、固定的な識別子の埋め込み操作を行うように処理してもよい。

【0085】つまり、分割部分に対する操作集合において、 $v_1 = (w_{1,1}(1$ つしか識別子埋め込み操作を用意しない))とすることで、 c_1 に対しては固定的操作を施すように処理してもよい。このときにも、 c_2, \dots, c_L のデータ量を c_1 のデータ量に比べて少なくとるように処理してもよい。

【0086】識別子を埋め込まないよりは、固定的なものであっても識別子を埋め込んだ方が好ましいので、コンテンツ配布用データのデータ量の削減を図りつつ、主体部について、固定的な識別子の埋め込み操作を行うように処理するのである。

【0087】(ロ) コンテンツ配布用データ送信部102の処理

コンテンツ配布用データ送信部102は、コンテンツ配布用データ格納部101に格納されるコンテンツ配布用データを全てのユーザ端末2に送信する処理を行う。すなわち、全てのユーザ端末2に対して、同じコンテンツ配布用データを送信する処理を行う。

【0088】(ハ) 鍵束生成部103の処理
鍵束生成部103は、図7の処理フローを実行することで、コンテンツの復号に用いられる鍵束を生成する処理を行う。

【0089】すなわち、先ず最初に、コンテンツ配布用データ生成部100から、コンテンツ配布用データの生成に用いられた各分割部分 c_i に対する鍵集合 k_i を取得する。

【0090】続いて、その取得した鍵集合 k_i からひとつ鍵 k_{i,j_i} を選択することを各 c_i について繰り返すことで、 $N_1 \times N_1 \times \dots \times N_L$ 個の鍵束 K_j

$K_j = k_{1,j_1}, k_{2,j_2}, \dots, k_{L,j_L}$ を作成する。ここで、 j_i は i ごとに異なる数である。

【0091】最後に、各鍵束ごとに、それにより埋め込まれる識別子 d_j を求めることで、鍵束と識別子との対応関係について記述する鍵束識別子対応リスト104を生成する。図2に例示するように、鍵束と識別子との対応関係を求めて、それに基づいて鍵束識別子対応リスト104を生成するのである。

【0092】このようにして生成される鍵束 K_j は、 Ω による c の各分割部分に識別子埋め込みと暗号化を行うことによって得られたデータに対する鍵を一つずつ含む。よって、鍵束 K_j によって、 c の各分割部分に対してある識別子を埋め込んだものの復号された形のデータが一つずつ得られることになる。

【0093】なお、管理情報として必要であれば、鍵束には、鍵束 K_j 中の各鍵がコンテンツ c のどの分割部分に対応するのかを示す鍵の対応情報を付属させる。鍵と分割部分との対応は、例えば、鍵束中の鍵に順序をつけ、これを分割部分の順序に対応させるといった手段をとることができる。

【0094】このようにして、鍵束の構成、つまり鍵束に含まれる鍵の構成によって、 c の全分割部分に埋め込まれた識別子の総体として得られる、復元されたコンテンツ c' の識別子の値が決定されることになる。

【0095】次に、鍵束識別子対応リスト104の生成処理について説明する。

【0096】鍵束 K_j によって埋め込まれるデータを d_j とする。つまり

$$d_j = R(\Omega'(w_j(\Omega(c))))$$

とする。ここで、 w_j は K_j に対応した識別子埋め込み操作である。

【0097】鍵束生成部103は、この対応関係に従って、各鍵束 K_j に対して埋め込まれた識別子 d_j を求め、その対応関係(K_j, d_j)のリストを生成することで、鍵束識別子対応リスト104を生成する。

【0098】(二) 識別子鍵束変換部105の処理後述するように、鍵束選択部106は、コンテンツに埋め込む識別子を選択し、鍵束識別子対応リスト104を参照することで、その識別子に対応付けられる鍵束を選択していくように処理する。

【0099】この処理のために、鍵束識別子対応リスト104が鍵束生成部103により生成されることになるが、この鍵束識別子対応リスト104が生成されない場

合には、識別子鍵束変換部105は、鍵束選択部106が選択した鍵束に対応付けられる鍵束を動的に特定する処理を行う。

【0100】埋め込まれる識別子が d であるとする。ここで、 d の値の決定に、鍵束中の各鍵によって暗号化されたコンテンツの分割部分に埋め込まれた情報が独立に影響する場合、つまり、 d の値から、それ自身以外の分割部分に埋め込まれた値に独立した形で、各分割部分に埋め込まれたデータを決定できる場合には、 i 番目の部分に埋め込まれた識別子 d_i は、ある関数 F_{d_i} によって、

$$d_i = F_{d_i}(d)$$

として求められる。この F_{d_i} は操作 R から求める。

【0101】最も簡単な例で説明するならば、コンテンツ c が4つに分割され、各分割部分に対して識別子0, 1を埋め込んで暗号化する場合にあって、 $d = 0101$ が与えられると、識別子鍵束変換部105は、その $d = 0101$ に対応付けられる鍵束が分割部分 c_1 に識別子0を埋め込み、分割部分 c_2 に識別子1を埋め込み、分割部分 c_3 に識別子0を埋め込み、分割部分 c_4 に識別子1を埋め込む鍵束であると特定する処理を行うのである。

【0102】(ホ) 鍵束選択部106の処理
鍵束選択部106は、あるユーザ U に対してコンテンツを配信する場合、図8(a)(b)の処理フローに従って、別に送信するコンテンツ配布用データ D の復号に用いる鍵束をユーザごとに選択する処理を行う。

【0103】すなわち、図8(a)の処理フローに従う場合には、各ユーザに対して事前にユーザID(u で表す)を発行しておくとともに、 u から流通コンテンツ識別子 d への変換を行う関数 $F_{user}(u)$ を用意しておいて、ユーザ端末2から、その発行したユーザIDを指定して鍵束の送信要求が発行されると、先ず最初に、そのユーザIDをその関数 F_{user} に代入することで、コンテンツに埋め込むべき識別子を求める。ここで、 u と d を同じ体系にしておけば $d = u$ となり、関数 F_{user} を省略できる。

【0104】続いて、鍵束識別子対応リスト104を参照することで、その識別子 d に対応付けられる鍵束 K を選択する。このとき、識別子鍵束変換部105に変換依頼を発行することで、その識別子 d に対応付けられる鍵束 K を特定するように処理することもある。

【0105】この選択した鍵束が鍵束送信部107により鍵束送信要求発行元のユーザ端末2に送信されることになるので、続いて、選択した鍵束を鍵束送信部107に通知するとともに、後述するコンテンツ違法コピーの検査処理のために、鍵束送信先のユーザのID(u)と、求めた識別子 d と、選択した鍵束 K との対応関係(u, d, K)を配布記録格納部108に保存する。

【0106】一方、図8(b)の処理フローに従う場合

には、ユーザ端末2から鍵束の送信要求が発行されると、先ず最初に、そのユーザに対して未発行の識別子 d を割り当てる。

【0107】続いて、鍵束識別子対応リスト104を参照することで、その識別子 d に対応付けられる鍵束 K を選択する。このとき、識別子鍵束変換部105に変換依頼を発行することで、その識別子 d に対応付けられる鍵束 K を特定するように処理することもある。

【0108】この選択した鍵束が鍵束送信部107により鍵束送信要求発行元のユーザ端末2に送信されることになるので、続いて、選択した鍵束を鍵束送信部107に通知するとともに、後述するコンテンツ違法コピーの検査処理のために、鍵束送信先のユーザのID(u)と、割り当てた識別子 d と、選択した鍵束 K との対応関係(u, d, K)を配布記録格納部108に保存する。

【0109】なお、コンテンツ違法コピーの検査処理の方法によっては、(u, d, K)を配布記録格納部108に保存するのではなくて、(u, d)または(u, K)を保存するように処理してもよい。また、このとき保存するユーザのID(u)としては、数字列のようなものばかりでなく、メールアドレスなどの別のシステムからユーザに与えられたものを用いてもよい。

【0110】(ヘ) 鍵束送信部107の処理
鍵束送信部107は、鍵束選択部106から通知される鍵束を暗号化して、鍵束要求発行元のユーザ端末2に送信する処理を行う。

【0111】コンテンツ配布用データが全てのユーザ端末2に一律に送信されるのとは異なって、鍵束については、ユーザに固有なものとして、各ユーザ端末2に1つずつそれぞれ異なるものが送信されることになる。

【0112】(ii) ユーザ端末2の処理の説明
(イ) コンテンツ配布用データ受信部200の処理
コンテンツ配布用データ受信部200は、コンテンツプロバイダ1から送信されてくるコンテンツ配布用データを受信して、コンテンツ配布用データ格納部201に格納する処理を行う。

【0113】(ロ) 鍵束受信部202は、コンテンツプロバイダ1から送信されてくる暗号化された鍵束を受信して、復号する処理を行う。

【0114】(ハ) コンテンツ復元部203の処理
コンテンツ復元部203は、図9の処理フローを実行することで、コンテンツプロバイダ1から送信されてきたコンテンツ配布用データからコンテンツを復元する処理を行う。

【0115】すなわち、コンテンツプロバイダ1からの鍵束 K_j (鍵束受信部202により復号される)を受け取ると、コンテンツ配布用データ格納部201から、復号対象のコンテンツ配布用データを読み出す。

【0116】続いて、受け取った鍵束 K_j から各分割部分 c_i に対応する鍵 k_{i,j_i} を取り出すとともに、復号対

象となるコンテンツ配布用データから、それらの各鍵 k_{i,j_i} に対応する暗号化された分割部分 $E(k_{i,j_i}, w_{i,j_i}(c_i))$ を取り出す。

【0117】続いて、各 $E(k_{i,j_i}, w_{i,j_i}(c_i))$ に対して、 k_{i,j_i} を適用して復号処理を行うことで $w_{i,j_i}(c_i)$ を復号する。

【0118】続いて、このようにして復号した $w_{i,j_i}(c_i)$ に対して結合操作 Ω' を適用して、コンテンツ c^w
 $c^w = \Omega'(w_{1,j_1}(c_1), w_{2,j_2}(c_2), \dots, w_{L,j_L}(c_L))$ を復元する。

【0119】このとき復元されるコンテンツには、コンテンツプロバイダ1から送信されてきた鍵束により指定されるユーザに固有の識別子が電子透かしの形で埋め込まれることになる。

【0120】(iii) コンテンツ違法コピー検査機関3の処理の説明

(イ) 識別子読出部300の処理

識別子読出部300は、検査対象となるコンテンツ(ユーザ端末2により復元されたコンテンツ)に埋め込まれている識別子を読み出す処理を行う。

【0121】(ロ) 取得部301の処理

取得部301は、コンテンツプロバイダ1の持つ配布記録格納部108の情報を取得して、それに基づいて、配布記録格納部302に対して、ユーザID(u)とそれに対応付けられる識別子 d との対応関係の情報を登録したり、配布記録格納部303に対して、ユーザID(u)とそれに対応付けられる鍵束 K との対応関係の情報を登録する処理を行う。

【0122】(ハ) 鍵束特定部304の処理

鍵束特定部304は、コンテンツプロバイダ1の備える識別子鍵束変換部105と同様の処理を実行することで、検査対象のコンテンツから読み出された識別子に対応付けられる鍵束を検出したり、コンテンツプロバイダ1の備える鍵束識別子対応リスト104を参照することで、検査対象のコンテンツから読み出された識別子に対応付けられる鍵束を検出する処理を行う。

【0123】(ニ) 違法コピー検査部305の処理

違法コピー検査部305は、検査対象のコンテンツが与えられると、図10の処理フローを実行することで、検査対象のコンテンツが違法コピーされたものであるのか否かを検査して、その検査結果を出力する処理を行う。

【0124】すなわち、先ず最初に、検査対象のコンテンツを所有するユーザのIDを入力する。続いて、識別子読出部300から、検査対象のコンテンツから読み出された識別子を受け取る。

【0125】続いて、その受け取った識別子をキーにして、配布記録格納部302(ユーザIDとそれに対応付けられる識別子 d との対応関係を管理)の情報を参照することで、検査対象のコンテンツの正規の所有者のユー

ザIDを特定する。

【0126】続いて、入力したユーザIDと、その特定した正規の所有者のユーザIDとが一致するの否かを判断することで、違法コピーが行われたの否かを検査して、その検査結果を出力する。

【0127】(ホ) 違法コピー検査部306の処理
違法コピー検査部306は、検査対象のコンテンツが与えられると、図11の処理フローを実行することで、検査対象のコンテンツが違法コピーされたものであるの否かを検査して、その検査結果を出力する処理を行う。

【0128】すなわち、先ず最初に、検査対象のコンテンツを所有するユーザのIDを入力する。続いて、識別子読出部300から読み出される識別子に応答して鍵束特定部304により特定される鍵束を、鍵束特定部304から受け取る。

【0129】続いて、その受け取った鍵束をキーにして、配布記録格納部303（ユーザIDとそれに対応付けられる鍵束Kとの対応関係を管理）の情報を参照することで、検査対象のコンテンツの正規の所有者のユーザIDを特定する。

【0130】続いて、入力したユーザIDと、その特定した正規の所有者のユーザIDとが一致するの否かを判断することで、違法コピーが行われたの否かを検査して、その検査結果を出力する。

【0131】このように構成される本発明について、その処理について具体的に説明すると、図2及び図3で説明したものとなる。

【0132】すなわち、本発明を具備するコンテンツプロバイダ1は、例えば、図2に示すように、コンテンツcをL個の(c₁, c₂, ..., c_L)に分割して、そのL個の各分割部分c_iに対して、例えば、電子透かし操作w_{i,j}を使って識別子“0”, “1”を埋め込んでから、暗号鍵k_{i,j}を使って暗号化することで、それらの暗号化コンテンツの集合で構成されるコンテンツ配布用データを生成するとともに、それらの暗号鍵k_{i,j}から、L個の各分割部分c_iごとに1つずつ暗号鍵k_{i,j}を選択することで、コンテンツcの復号に用いられる鍵束K_j (j=1~2^L)を生成する。

【0133】このとき、本発明を具備するコンテンツプロバイダ1は、鍵束K_jと、それにより復号されるコンテンツから読み出される識別子d_j（図2の例では“0”か“1”の羅列データ）との対応関係について記述する鍵束識別子対応リスト104を生成する。

【0134】続いて、本発明を具備するコンテンツプロバイダ1は、図3に示すように、全てのユーザ端末2-iに対して、生成したコンテンツ配布用データを配布するとともに、各ユーザ端末2-iに対して、1つずつ鍵束K_jを選択して、その選択した鍵束K_jの暗号化したものを配布する。

【0135】この鍵束K_jの選択処理は、例えば、配布

先ユーザのIDを関数F_{user}(u)に代入することで識別子を得て、それをキーにして鍵束識別子対応リスト104を参照することで行ったり、未発行の識別子を選択し、それをキーにして鍵束識別子対応リスト104を参照することで行う。

【0136】ここで、鍵束識別子対応リスト104が生成されていないときには、識別子を指定して、識別子鍵束変換部105に対して変換依頼を発行することで、識別子に対応付けられる鍵束を得るように処理する。

【0137】このような配布処理を行うときに、本発明を具備するコンテンツプロバイダ1は、本発明を具備するコンテンツ違法コピー検査機関3によりコンテンツ違法コピー検査を可能ならしめるために、図3に示すように、その配布記録として、鍵束送信先のユーザのID(u)と、割り当てた識別子dと、選択した鍵束Kとの対応関係(u, d, K)を配布記録格納部108に保存する。

【0138】一方、本発明を具備するユーザ端末2は、本発明を具備するコンテンツプロバイダ1から配布される鍵束を受けて、受信してあるコンテンツ配布用データから、その鍵束を構成する各暗号鍵に対応付けられる暗号化コンテンツ部分を取り出し、その取り出した暗号化コンテンツ部分を、それに対応付けられる暗号鍵（復号鍵）で復号して、その復号したコンテンツ部分を統合することでコンテンツを復元する。

【0139】このようにして復元されるコンテンツには、配布される鍵束に従って、配布先ユーザに固有な電子透かし情報が埋め込まれることになる。しかも、この配布先ユーザに固有の電子透かし情報の埋め込みは、配布先のユーザ側で行われることになる。

【0140】一方、本発明を具備するコンテンツ違法コピー検査機関3は、検査対象のコンテンツが与えられると、そのコンテンツに埋め込まれる識別子を読み取り、それをキーにして、本発明を具備するコンテンツプロバイダ1が保存する配布記録の情報を参照することで、検査対象のコンテンツの正規の配布先ユーザを特定して、それに従って、検査対象のコンテンツを所有するユーザが正規のコンテンツ所有者であるの否かを検査する。

【0141】このようにして検査されるコンテンツには、正規のコンテンツ所有者に固有の識別子が埋め込まれており、これにより、コンテンツ所有者が正規の所有者であるの否かということと、コンテンツの不正コピーが行われた場合には、どの正規のコンテンツ所有者の所有するコンテンツからコピーが行われたのかということを検出できるようになる。

【0142】このようにして、本発明では、ユーザ側で、ユーザに固有な電子透かし情報をコンテンツに埋め込むという形態をとりつつ、そのとき埋め込む電子透かし情報とその埋め込み処理とについては、実際には鍵束を使って提供側で制御するようしており、これによ

り、ユーザ側で、電子透かし情報の埋め込みを不正にキャンセルしたり、偽の電子透かし情報が埋め込まれることを防止できるようになる。

【0143】そして、コンテンツの不正コピーが行われる場合に、それを正確に検出できるとともに、そのコピー元を正確に検出できるようになる。

【0144】

【実施例】（１）静止画像データに対するコンテンツ配布用データ生成

（イ）〔分割操作 Ω 〕

静止画像データを縦横 $n \times m$ の格子状に分割し、 $n \times m$ 個の部分に分割部分とする。この操作を分割操作 Ω とする。

【0145】結合操作 Ω' は、 $n \times m$ 個の部分に元の位置に並べて元のサイズの画像とするものである。この際に、符号化パラメータなどのヘッダ情報が符号化方式 F のデータに存在する場合は、各分割部分のデータにこの値を受け継ぎ、結合時にパラメータを復元する。

【0146】JPEG画像においては、 8×8 画素のブロックに分割して、ブロック毎に圧縮符号化が行われる。これから、格子状に分割する場合には、格子の縦横の画素数をブロックの画素数の倍数にして、画像を $n' \times m'$ ブロックからなる矩形領域に分割する。

【0147】（ロ）〔識別子埋め込み操作 W 〕

各分割部分に対して、画像への電子透かし埋め込み方式を用いて識別子を埋め込む。電子透かし方式は埋め込みデータを指定することで、同一アルゴリズムで複数のデータの埋め込みが可能である。この操作を識別子埋め込み操作 W とする。

【0148】つまり、各 $w_{i,j}$ は、共通の透かしアルゴリズム w によって、あるデータ $d_{i,j}$ を電子透かしでコンテンツに埋め込む操作として実現する。 $d_{i,j}$ は $j \neq j'$ のとき $d_{i,j} \neq d_{i,j'}$ となるようにとる。読み取り関数 R は W から自然に定義される。

【0149】（ハ）〔暗号化〕

識別子を埋め込まれたコンテンツの分割部分に対して、実施形態例で説明したような暗号化を適用する。

【0150】（２）動画データに対するコンテンツ配布用データ生成

（イ）〔分割操作 Ω 〕

MPEG符号化された動画データにおいて、Pピクチャ、Bピクチャにおける動き補償ベクトルを符号化した部分をフレームごとに取り出し、最初のフレームから取り出したものを分割部分 c_2 、次のフレームから取り出したものを分割部分 c_3 というように、 $L-1$ 個の調整部が存在する場合に、 $L-1$ フレーム周期で動き補償ベクトル符号化部分を分割部分に割り当てる。

【0151】また、元のコンテンツ c の符号化データから動き補償ベクトルを符号化した部分を取り除いたデータを主体部 c_1 とする。

【0152】結合操作 Ω' は、 Ω と逆に、主体部 c_1 から調整部を取り除いたのと逆の手続きで動き補償ベクトルを c_1 に追加することで行う。

【0153】（ロ）〔識別子埋め込み〕

調整部 c_k に割り当てられた動き補償ベクトルを、埋め込む値にしたがって変位を加える。

【0154】（ハ）〔暗号化〕

識別子を埋め込まれたコンテンツの分割部分に対して、実施形態例で説明したような暗号化を適用する。

【0155】（３）流通方式（会員登録あり）

コンテンツ c の所有者は、配布用コンテンツ作成および配布を行うためのセンタにコンテンツを預ける。

【0156】センタは、分割操作 Ω 、識別子埋め込み操作 W 、分割部分の暗号化を行ってコンテンツ配布用データ D を作成する。

【0157】センタは、コンテンツ配布用データ D を配布する。ここでの配布方式としては、CD-ROMに焼き付けて物流によって配送、インターネット上のデータサーバからのダウンロード、放送波による配信、電子メールによる配信など、任意のデータ配送手段を用いてよい。

【0158】ユーザは、配布されたコンテンツ配布用データ D を入手する。ユーザは、配布されたコンテンツ配布用データ D を復号して、コンテンツ c を復元するための鍵束をセンタに要求する。この要求時に、ユーザは、復号したいコンテンツと、センタに登録してあるユーザIDとをセンタに送信する。

【0159】センタは、ユーザIDに対応した鍵束 K を用意する。鍵束 K の用意の方法としては、実施形態例に述べた方法に基づいて行う。センタは、この用意した鍵束 K をユーザに送付する。

【0160】鍵束 K の送付については、一般的な鍵配送方式を用いる。これらの方式の一つとして、鍵束 K を配送用の鍵 k で暗号化して送付する方式がある。別の方式としては、さらに鍵 k をユーザの公開鍵 K_U で暗号化して、鍵束 K に加えて鍵 k をユーザに送付する方法がある。Infoket が鍵配送の代表的例である。

【0161】ユーザは、鍵束 K を受信し、実施形態例で説明した「コンテンツの復元法」に基づいて：コンテンツ c^W を復元する。ここで、 c^W は識別子を埋め込まれたコンテンツである。

【0162】（４）流通方式（会員登録なし）

コンテンツ c の所有者は、配布用コンテンツ作成および配布を行うためのセンタにコンテンツを預ける。

【0163】センタは、分割操作 Ω 、識別子埋め込み操作 W 、分割部分の暗号化を行ってコンテンツ配布用データ D を作成する。

【0164】センタは、コンテンツ配布用データ D を配布する。ここでの配布方式としては、CD-ROMに焼き付けて物流によって配送、インターネット上のデータ

サーバからのダウンロード、放送波による配信、電子メールによる配信など、任意のデータ配送手段を用いてよい。

【0165】ユーザは、配布されたコンテンツ配布用データDを入手する。ユーザは、配布されたコンテンツ配布用データDを復号して、コンテンツcを復元するための鍵束をセンタに要求する。この要求時に、ユーザは、復号したいコンテンツと、センタの外部に存在する認証機関から入手した認証データとをセンタに送信する。

【0166】センタは、ユーザIDに対応した鍵束Kを用意する。鍵束Kの用意の方法としては、実施形態例に述べた方法に基づいて行う。センタは、この用意した鍵束Kをユーザに送付する。

【0167】ユーザは、鍵束Kを受信し、実施形態例で説明した「コンテンツの復元法」に基づいて、コンテンツc^wを復元する。ここで、c^wは識別子を埋め込まれたコンテンツである。

【0168】(5) 静止画像の場合の例

(イ) データの作成

N×M画素の画像をn×m個のブロックに分割し、C₁, C₂, ..., C_{n×m}とする。各C_iは、(N/n)×(M/m)画素のブロックである。

【0169】この(N/n)×(M/m)画素のブロックに対する電子透かし埋め込みW₁, W₂, ..., W_xを用意する。これは、ブロックに、それぞれ異なる値w₁, w₂, ..., w_xを埋め込む操作を行う。

【0170】W_jによって透かしを埋め込まれたブロックC_iをW_j(C_i)と書くことにすると、各C_iに対してすべてのW_jを適用することで、W₁(C₁), W₂(C₁), ..., W_x(C₁), W₂(C₂), ..., W_x(C_{n×m})

というx×n×m個のデータができる。

【0171】これを、それぞれ異なる鍵k_{ji}で暗号化して、

E(k_{1,1}, W₁(C₁)), E(k_{2,1}, W₂(C₁)), ..., E(k_{x,n×m}, W_x(C_{n×m}))

というx×n×m個のデータを作成し、これをCD-R OMなどに格納して配送する。

【0172】(ロ) 鍵の送信

コンテンツプロバイダは、i=1, 2, 3, ..., n×mのそれぞれについて、鍵k_{ji}を選択し、鍵束K=(k_{j1,1}, k_{j2,2}, ..., k_{jn×m,n×m})を作成する。

【0173】(ハ) 復元

ユーザは、鍵束Kを受け取り、その受け取った鍵束K中の各鍵k_{ji}を使って、対応する暗号化された透かし入りブロックE(k_{ji,i}, W_j(C_i))を復号することで、

W_{j1}(C₁), W_{j2}(C₂), ..., W_{jn×m}(C_{n×m})

を得て、それを統合することで画像を復元する。

【0174】これらのブロックを再構成してできたN×M画素の静止画像には、

w_{j1}, w_{j2}, ..., w_{jn×m}

というデータが透かしとして入っていることになる。

【0175】(6) 違法コピー検査の効果

違法コピーを検査する機関は、検査対象となるコンテンツc^wに対し、データ読み取り操作Rを適用して識別子d=R(c^w)を取得する。

【0176】ここで、dは、コンテンツc^wの元となったコンテンツcを配布したユーザを識別する情報となっている。

【0177】違法コピーを検査する機関は、センタで管理している識別子と鍵束との対応に基づき、読み出したデータdから、コンテンツc^wの配布先のユーザUを特定する。

【0178】コンテンツc^wを実際に所持していたユーザU'と、特定したユーザUとが異なった場合、コンテンツc^wは最初の配布先とは異なるユーザに所持されていたことを示す。

【0179】この機能によって、あるユーザに所持されたコンテンツが違法コピーされたものかどうかを判断できるようになるとともに、違法コピーが元々どのユーザに配布されたものかを検出できる。

【0180】(7) 透かしのチェック効果

本発明で配布されたコンテンツc^wに対する識別子の検査を次のように行うことで、透かしをチェックする。

【0181】コンテンツからのデータ読み取り操作Rによって、識別子d=R(c^w)を読み出す。

【0182】このdは、鍵束K

K_j=k_{1,j1}, k_{2,j2}, ..., k_{L,jL}

に対応した透かし埋め込み操作

w_j=w_{1,j1}, w_{2,j2}, ..., w_{L,jL}

に一意に対応し、K_jの組み合わせが異なると、読み出されるデータdは異なる。

【0183】よって、Rによって読み出されたdから、どの鍵束が適用されてコンテンツが復元されたかが識別できる。

【0184】鍵束管理側では、鍵束Kまたは識別子dとユーザUとの対応が管理されている。(U, d)または(U, K)または(U, d, K)が管理されている場合、dまたはKからUを知ることができる。

【0185】d=F_{user}(u)としてdを決定した場合は、F_{user}の逆関数F_{user}⁻¹を用いてdからuを得ることができる。

【0186】これにより、あるユーザに所持されたコンテンツが違法コピーされたものかどうかを判断できるようになるとともに、違法コピーが元々どのユーザに配布されたものかを検出できる。

【0187】(8) データ量削減の効果

本発明では、コンテンツ配布用データに復号鍵を適用す

ること得られる互いに異なる識別子をもつコンテンツは $N_1 \times N_2 \times \dots \times N_L$ 種類生成される。

【0188】元のコンテンツのデータ量を s 、分割部分 c_1, c_2, \dots, c_L のデータ量を s_1, s_2, \dots, s_L とすると、 c を分割せずに $N_1 \times N_2 \times \dots \times N_L$ 種類の異なる識別子をもつコンテンツを生成する場合、合計のデータ量は、

$$S = N_1 \times N_2 \times \dots \times N_L \times s$$

である。

【0189】これに対して、本発明による配布用データのサイズは、およそ

$$S' = N_1 \times s_1 + N_2 \times s_2 + \dots + N_L \times s_L$$

である。

【0190】 $s \approx s_1 + s_2 + \dots + s_L$ であることから、 $S \gg S'$ となり、本発明によれば、非常に少ないデータ量で、多くの識別子を持ったコンテンツを同一の配布用データ内に用意できることになる。これは、CD-ROMなどによる同一コンテンツの大量流通に適している。

【0191】特に、 N_k の値が大きいものほど、 s_k を小さくすれば S' はそれだけ小さくなる。

【0192】分割部分を主体部と調整部とにクラス分けした場合は、主体部のデータ量を多くとり、各調整部を少ないデータ量で構成される分割部分とすることで、このデータ削減効果は更に大きなものとなる。

【0193】図示実施形態例に従って本発明を説明したが、本発明はこれに限定されるものではない。例えば、実施形態例では、1つの電子透かし方式を使って、異なる電子透かし情報をコンテンツに埋め込むという構成を採ったが、コンテンツの分割部分毎に、その分割部分のコンテンツ属性に合った電子透かし方式を用いるという構成を用いることも可能である。

【0194】

【発明の効果】以上説明したように、本発明では、ユーザ側で、ユーザに固有な電子透かし情報をコンテンツに埋め込むという形態をとりつつ、そのとき埋め込む電子透かし情報とその埋め込み処理については、実際には鍵束を使って提供側で制御するようにしており、これにより、ユーザ側で、電子透かし情報の埋め込みを不正にキャンセルしたり、偽の電子透かし情報が埋め込まれることを防止できるようになる。

【0195】そして、コンテンツの不正コピーが行われる場合に、それを正確に検出できるとともに、そのコピー元を正確に検出できるようになる。

【0196】以上に説明したように、本発明では、コンテンツを複数の部分に分割して、それぞれの分割部分に対して複数の電子透かしを用意し、個々のユーザに対する電子透かしを、抽出された分割部分の電子透かしの値の組み合わせとするという構成を採っており、これにより、電子透かし入りコンテンツとして用意すべきデータ

量を少なくできるようになる。

【0197】すなわち、従来行われていたように、コンテンツに直接、利用者情報を電子透かしとして埋め込む場合、 n 人の利用者に対しては n 通りに電子透かしを埋め込む必要があり、提供者での電子透かし埋め込み回数は n 回となる。元のコンテンツのデータ量を C とすると、電子透かしによるデータ量増加がないと仮定しても、電子透かし入りコンテンツのデータ量の合計は $C \times n$ である。これでは、利用者が増加するにつれて、膨大な埋め込み回数になるとともに、膨大なデータ量になる。

【0198】このように、従来技術に従っていると、電子透かし埋め込み回数の問題から、提供者の負荷が大きく、また、データ量の問題から、予め用意したコンテンツのCD-ROMや放送などによる一括の配布が不可能となっている。

【0199】これに対して本発明の方式では、コンテンツから m 個の部分抽出し、各部分に k 種類の電子透かしデータを対応させる場合、コンテンツ全体で k^m 種類の電子透かしが埋め込める。 n 人の利用者に対しては、およそ、「 $k \times \log n \div \log k$ 」回の電子透かし埋め込みとなり、 n に比べて非常に少ない。また、 n 人の利用者すべてを区別する電子透かしの組み合わせを実現するためのデータ量も、これに比例するため、 $C \times n$ に比べて非常に少ない。

【0200】さらに、抽出部分の合計 C' （本発明の電子透かし埋め込み処理の対象となる部分の合計）をコンテンツのデータ量 C に比べて小さくとると、異なる利用者のための電子透かしを埋め込んだデータを予め用意するためのデータ量が「 $C' \times \log n \div \log k$ 」となり、オリジナルコンテンツ C に比べて n 人の利用者用の電子透かし情報追加のためのデータ量が小さく、予め全利用者用の電子透かし入りコンテンツを用意してCD-ROMなどによる一括配布や、放送やサーバからのダウンロードによる一括配布などが可能となる。

【図面の簡単な説明】

【図1】本発明を具備するシステムの構成の一例である。

【図2】本発明の処理の一例である。

【図3】本発明の処理の一例である。

【図4】本発明の一実施形態例である。

【図5】本発明の一実施形態例である。

【図6】コンテンツ配布用データ生成部の実行する処理フローの一実施形態例である。

【図7】鍵束生成部の実行する処理フローの一実施形態例である。

【図8】鍵束選択部の実行する処理フローの一実施形態例である。

【図9】コンテンツ復元部の実行する処理フローの一実施形態例である。

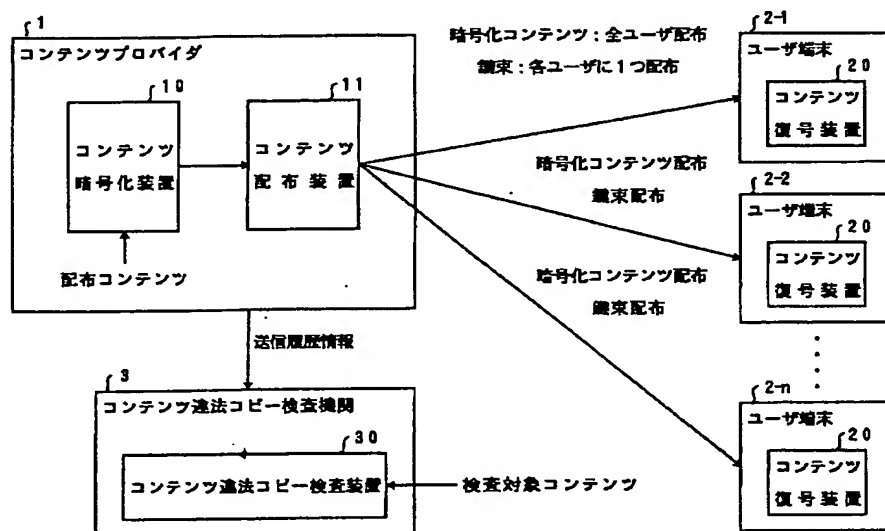
【図10】違法コピー検査部の実行する処理フローの一実施形態例である。

【図11】違法コピー検査部の実行する処理フローの一実施形態例である。

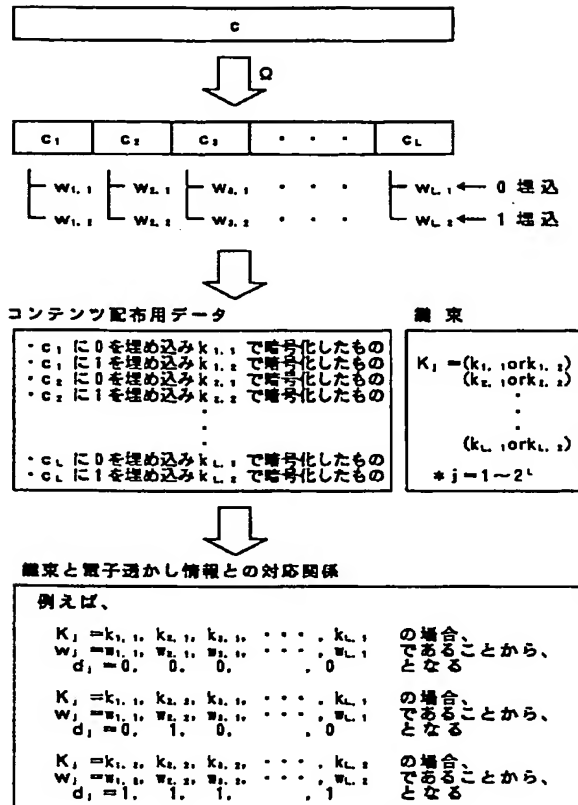
【符号の説明】

- | | | | |
|-----|----------------|-----|----------------|
| 1 | コンテンツプロバイダ | 104 | 鍵束識別子対応リスト |
| 2 | ユーザ端末 | 105 | 識別子鍵束変換部 |
| 3 | コンテンツ違法コピー検査機関 | 106 | 鍵束選択部 |
| 10 | コンテンツ暗号化装置 | 107 | 鍵束送信部 |
| 11 | コンテンツ配布装置 | 108 | 配布記録格納部 |
| 20 | コンテンツ復号装置 | 200 | コンテンツ配布用データ受信部 |
| 30 | コンテンツ違法コピー検査装置 | 201 | コンテンツ配布用データ格納部 |
| 100 | コンテンツ配布用データ生成部 | 202 | 鍵束受信部 |
| 101 | コンテンツ配布用データ格納部 | 203 | コンテンツ復元部 |
| 102 | コンテンツ配布用データ送信部 | 300 | 識別子読出部 |
| 103 | 鍵束生成部 | 301 | 取得部 |
| | | 302 | 配布記録格納部 |
| | | 303 | 配布記録格納部 |
| | | 304 | 鍵束特定部 |
| | | 305 | 違法コピー検査部 |
| | | 306 | 違法コピー検査部 |

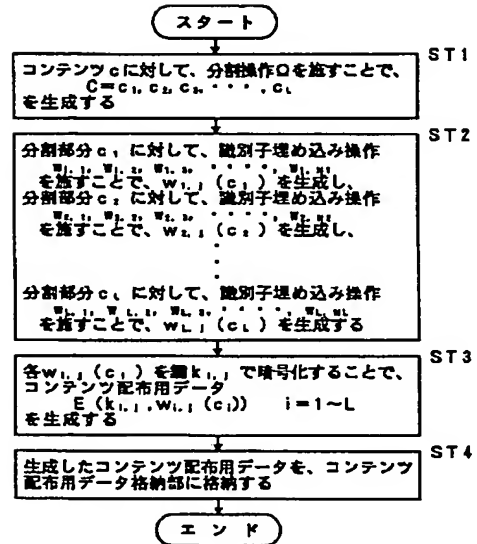
【図1】



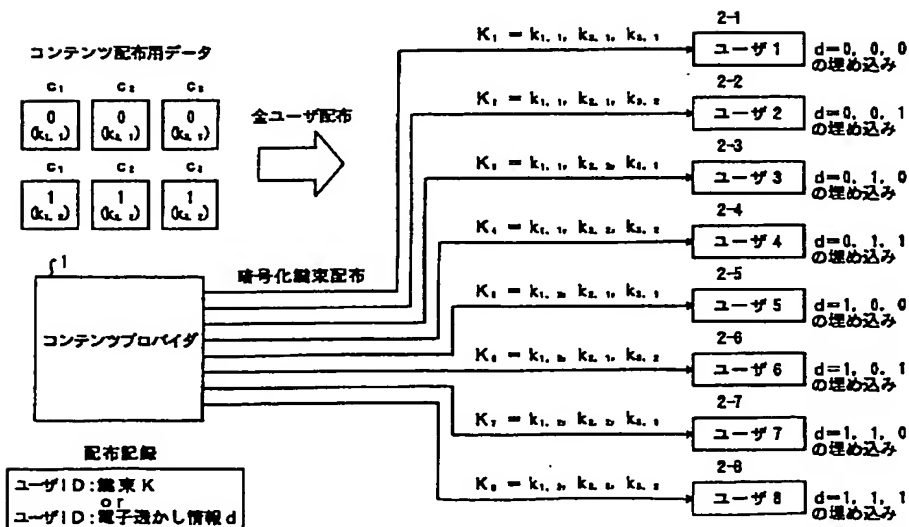
【図2】



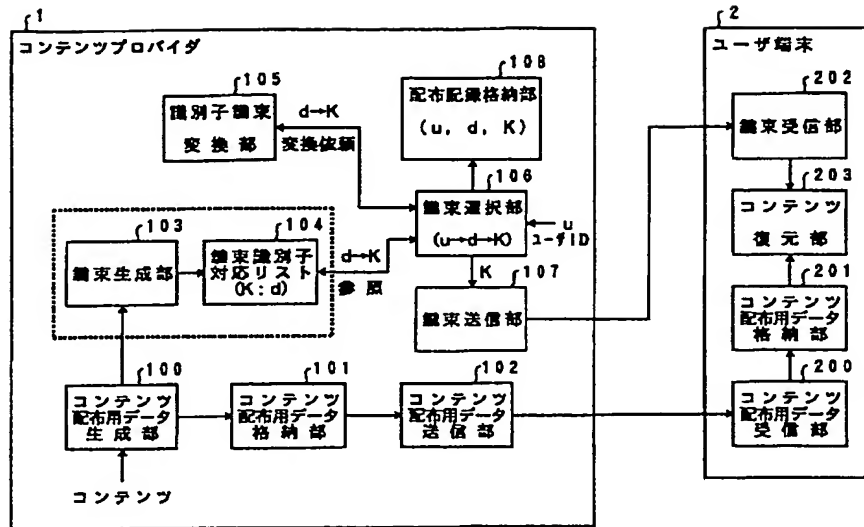
【図6】



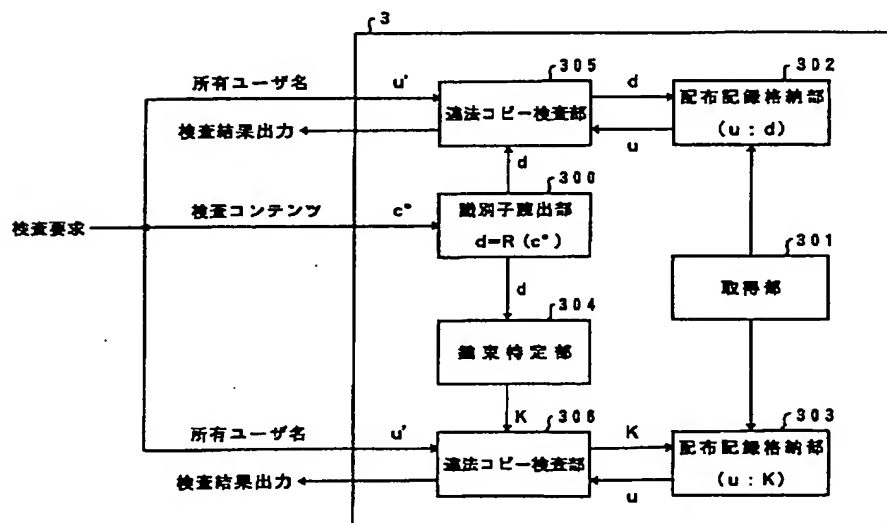
【図3】



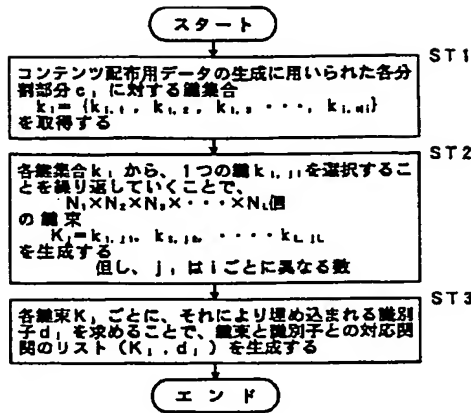
【図 4】



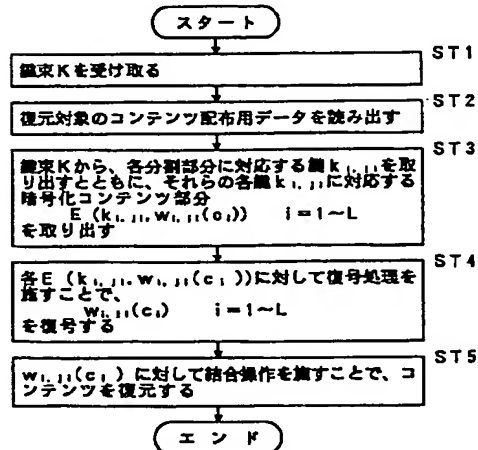
【図 5】



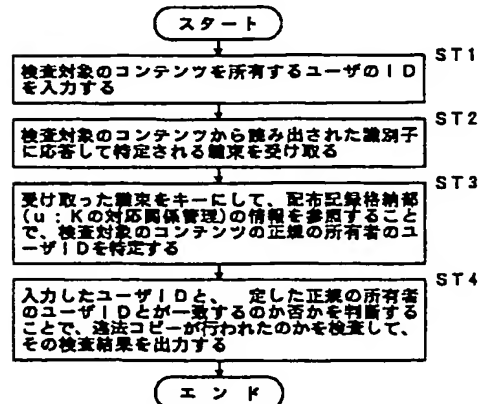
【図7】



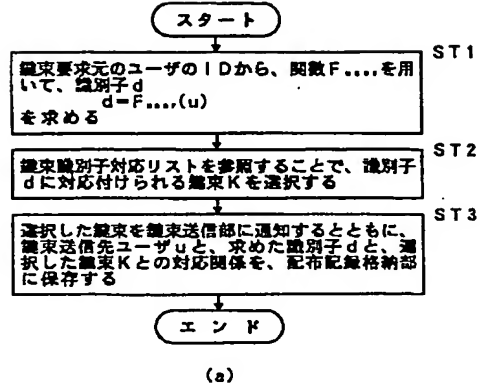
【図9】



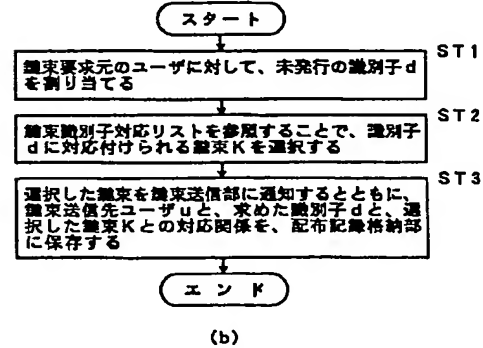
【図11】



【図8】

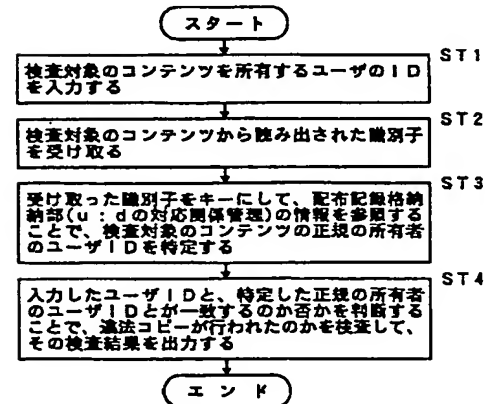


(a)



(b)

【図10】



フロントページの続き

(51) Int. Cl.⁷ 識別記号 F I テーマコード (参考)
// H O 4 N 7/167

Fターム(参考) 5C063 AB05 CA23 DA20 DB09
5C064 BA07 BB02 BB05 BC06 BC18
BC20 BC23 BD08 BD09
5J104 AA01 AA14 AA16 EA01 EA04
NA02

(54) 【発明の名称】 コンテンツ暗号化方法及び装置と、コンテンツ復号方法及び装置と、コンテンツ配布方法及び装置と、コンテンツ違法コピー検査方法及び装置と、コンテンツ暗号化プログラム及びそのプログラムの記録媒体と、コンテンツ復号プログラム及びそのプログラムの記録媒体と、コンテンツ配布プログラム及びそのプログラムの記録媒体と、コンテンツ違法コピー検査プログラム及びそのプログラムの記録媒体